REMARKS

This paper is responsive to a Non-Final Office action dated November 16, 2006. Claims 1-22 and 25-56 were examined. Claims 4, 17, 25-32, 36, and 44 stand rejected under 35 U.S.C. § 112, second paragraph. Claims 1-8, 14-27, 33-39, 41-51, and 53-56 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U. S. Publication No. 2002/0094081 to Medvinsky in view of U.S. Patent No. 6,819,766 to Weidong. Claims 9-13, 28-32, 40, and 52 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Medvinsky in view of Weidong, and further in view of U.S. Patent No. 7,110,546 to Staring.

Drawings

Applicants respectfully request the Examiner to indicate acceptance of the Replacement Sheet filed on August 23, 2006.

Claim Rejections Under 35 U.S.C. § 112, second paragraph

Claims 4, 17, 25-32, 36, and 44 stand rejected under 35 U.S.C. § 112, second paragraph. Claims 4, 17, 25, 36, and 44 are canceled. Claim 26 is amended to depend from claim 22. Applicants believe that the pending claims satisfy the requirements of 35 U.S.C. § 112, second paragraph. Accordingly, Applicants respectfully request that the rejection under 35 U.S.C. § 112, second paragraph be withdrawn.

Claim Rejections Under 35 U.S.C. § 103

Claims 1-8, 14-27, 33-39, 41-51, and 53-56 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U. S. Publication No. 2002/0094081 to Medvinsky (hereinafter, "Medvinsky") in view of U.S. Patent No. 6,819,766 to Weidong (hereinafter, "Weidong").

Regarding claim 1, Applicants respectfully maintain that Medvinsky, alone or in combination with Weidong or other references of record, fails to teach or suggest

> selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet,

as required by claim 1. Medvinsky teaches that

> processor 124 coordinates with key stream generator 122 to begin generating a key stream based on a single key. Upon generation of the key stream, encryptor 118 encrypts each voice packet using the key stream. As noted, time stamps are employed to perform synchronization so the voice packets are recoverable at the remote end. Each voice packet includes an RTP time stamp used as a pointer to the key stream. Encryptor 118 employs the RTP time stamp to calculate an index into the key stream, and thereafter, calls key stream generator 122 to get the appropriate key stream bytes for encryption.

Paragraph 0033. Nowhere does Medvinsky teach or suggest selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet, as required by claim 1.

Weidong fails to compensate for the shortcomings of Medvinsky. Weidong teaches generating a session key, generating a key encryption key based on an initial vector, and generating a set of indices by a one-way transform mapping based on the length of the binary representation of the encrypted session key, the length of the binary representation of the encrypted data, and the initial vector. Col. 2, lines 39-61. Wiedong teaches regenerating the set of indices by using the one-way transform mapping based on the length of the binary representation of the encrypted session key, the length of the binary representation of the encrypted data, and the initial vector, rebuilding the encrypted session key by using the regenerated set of indices, regenerating the key encryption key, using the initial vector, and regenerating the session key by decrypting the rebuilt encrypted session key using the regenerated key encryption key. Col. 2, line 62-col. 3, line 17. Weidong fails to teach a continuous decryption stream, as required by claim 1, but rather teaches a set of indices based on a vector, which may be input by a user. Col. 7, lines 31-35. Nowhere does Weidong teach or suggest a fixed length segment of a continuous decryption key stream, as required by claim 1.

Since neither Medvinsky nor Weidong discloses or suggests the recited limitation and no other art of record adds the missing disclosure, accordingly, Applicants respectfully request that the rejection of claim 1 and all claims dependent thereon, be withdrawn.

Regarding claim 20, Applicants respectfully maintain that Medvinsky, alone or in combination with Weidong or other references of record, fails to teach or suggest

> forming the at least a portion of the message digest value by truncating the message digest value,

as required by claim 20. The Office relies on paragraphs 0054-0057 of Medvisnky to supply this teaching. That portion of Medvinsky teaches a Message Authentication Code (MAC) algorithm change. The MAC algorithm change, alone or in combination with other portions of Medvinsky or other references of record, fails to expressly teach or suggest truncating a locally generated message digest value to form a truncated message digest, as required by claim 20. The Office implies that the MAC algorithm change of Medvinsky inherently teaches the limitations of claim 20.

Applicants respectfully point out that while a teaching may be express or inherent, inherency is a stringent standard.

> To establish inherency, the extrinsic evidence "must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill." *Continental Can Co. v. Monsanto Co.*, 948 F.2d 1264, 1268, 20 U.S.P.Q.2D (BNA) 1746, 1749 (Fed. Cir. 1991). "Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient." Id. at 1269, 20 U.S.P.Q.2D (BNA) at 1749 (quoting *In re Oelrich*, 666 F.2d 578, 581, 212 U.S.P.Q. 323, 326 (C.C.P.A. 1981).

See In re Robertson, 169 F.3d 743, 745; 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999); MPEP § 2112.IV. Applicants disagree that it is inherent for the system of Medvinsky to practice the claim. For example, there is no teaching or suggestion that the MAC algorithm change of Medvinsky must (or does) form the at least a portion of the message digest value by truncating the message digest value, as required by claim 20. To be inherent in forming the at least a portion of the message digest value by truncating the message digest value, that function must by necessity be performed in Medvinsky. It is not.

Since Medvinsky does not expressly or inherently disclose or suggest the recited limitation and no other art of record adds the missing disclosure, accordingly, Applicants respectfully request that the rejection of claim 20 and all claims dependent thereon, be withdrawn.

Regarding claim 33, Applicants respectfully maintain that Medvinsky, alone or in combination with Weidong or other references of record, fails to teach or suggest

> a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold,

as required by claim 33. Medvsinky teaches synchronization by directing key stream generator 132 to output the same key stream bytes from the same key stream used to encrypt the data. Paragraph 0034. Medvinsky teaches N, which is a counter that holds the number of times that a time stamp has wrapped around. Paragraph 0042. Nowhere does Medvinsky expressly teach a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold, as required by claim 33. The Office implies that the synchronization of the stream cipher using a time stamp of Medvinsky and the counter value N of Medvinsky each inherently teach the limitations of claim 33.

Applicants respectfully point out that while a teaching may be express or inherent, inherency is a stringent standard. See In re Robertson, 169 F.3d 743, 745; 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999); MPEP § 2112.IV. Applicants disagree that it is inherent for the system of Medvinsky to practice the claim. For example, there is no teaching or suggestion that the synchronization techniques of Medvinsky must (or do) determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold, as required by claim 33. To be inherent in determining if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold, those functions must by necessity be performed in Medvinsky. They are not.

Since Medvinsky does not expressly or inherently disclose or suggest the recited limitation and no other art of record adds the missing disclosure, accordingly, Applicants respectfully request that the rejection of claim 33 and all claims dependent thereon, be withdrawn.

Regarding claim 54, Applicants respectfully maintain that Medvinsky, alone or in combination with Weidong or other references of record, fails to teach or suggest,

> padding the payload to a given size with padding, the given size corresponding to the fixed length segment size, wherein the fixed length segment of the continuous decryption key is applied to the padded payload, a remaining portion of the fixed length segment being applied to the padding,

as required by claim 54. Medvinsky fails to teach or suggest padding as required by claim 54. The Office relies on Weidong to supply this teaching. Weidong teaches padding data for encryption. Col. 9, lines 10-24. Weidong teaches removing padding to decrypt the encrypted data. Col. 9, lines 25-40. However, nowhere does Weidong teach or suggest applying the fixed length segment of the continuous decryption key applied to the padded payload, a remaining portion of the fixed length segment being applied to the padding, as required by claim 54. Accordingly, Applicants respectfully request that the rejection of claim 54, be withdrawn.

Regarding claim 14, Applicants respectfully maintain that Medvinsky, alone or in combination with Weidong or other references of record, fails to teach or suggest

> selecting a fixed length segment of a continuous encryption key stream,

as required by claim 14. Medvinsky teaches that

> processor 124 coordinates with key stream generator 122 to begin generating a key stream based on a single key. Upon generation of the key stream, encryptor 118 encrypts each voice packet using the key stream. As noted, time stamps are employed to perform synchronization so the voice packets are recoverable at the remote end. Each voice packet includes an RTP time stamp used as a pointer to the key stream. Encryptor 118 employs the RTP time stamp to calculate an index into the key stream, and thereafter, calls key stream generator 122 to get the appropriate key stream bytes for encryption.

Paragraph 0033. Nowhere does Medvinsky teach or suggest selecting a fixed length segment of a continuous encryption key stream, as required by claim 1.

Weidong fails to compensate for the shortcomings of Medvinsky. Weidong teaches generating a session key, generating a key encryption key based on an initial vector, and generating a set of indices by a one-way transform mapping based on the length of the binary representation of the encrypted session key, the length of the binary representation of the encrypted data, and the initial vector. Col. 2, lines 39-61. Wiedong teaches regenerating the set of indices by using the one-way transform mapping based on the length of the binary representation of the encrypted session key, the length of the binary representation of the encrypted data, and the initial vector, rebuilding the encrypted session key by using the regenerated set of indices, regenerating the key encryption key, using the initial vector, and regenerating the session key by decrypting the rebuilt encrypted session key using the regenerated key encryption key. Col. 2, line 62-col. 3, line 17. Weidong fails to teach a continuous encryption key stream, as required by claim 14, but rather teaches a set of indices based on a vector, which may be input by a user. Col. 7, lines 31-35. Nowhere does Weidong teach or suggest a fixed length segment of a continuous encryption key stream, as required by claim 14.

Since neither Medvinsky nor Weidong discloses or suggests the recited limitation and no other art of record adds the missing disclosure, accordingly, Applicants respectfully request that the rejection of claim 14 and all claims dependent thereon, be withdrawn.

Regarding claim 41, Applicants respectfully maintain that Medvinsky, alone or in combination with Weidong or other references of record, fails to teach or suggest

> an encryption engine configured to apply a portion of a fixed length segment of a continuous encryption key stream to data to form an encrypted payload,

as required by claim 41. Medvinsky teaches that

> processor 124 coordinates with key stream generator 122 to begin generating a key stream based on a single key. Upon generation of the key stream, encryptor 118 encrypts each voice packet using the key stream. As noted, time stamps are employed to perform synchronization so the voice packets are recoverable at the remote end. Each voice packet includes an RTP time stamp used as a pointer to the key stream. Encryptor 118 employs the RTP time stamp to calculate an index

> into the key stream, and thereafter, calls key stream generator 122 to get the appropriate key stream bytes for encryption.

Paragraph 0033. Nowhere does Medvinsky teach or suggest a fixed length segment of a continuous encryption key stream, as required by claim 41.

Weidong fails to compensate for the shortcomings of Medvinsky. Weidong teaches generating a session key, generating a key encryption key based on an initial vector, and generating a set of indices by a one-way transform mapping based on the length of the binary representation of the encrypted session key, the length of the binary representation of the encrypted data, and the initial vector. Col. 2, lines 39-61. Wiedong teaches regenerating the set of indices by using the one-way transform mapping based on the length of the binary representation of the encrypted session key, the length of the binary representation of the encrypted data, and the initial vector, rebuilding the encrypted session key by using the regenerated set of indices, regenerating the key encryption key, using the initial vector, and regenerating the session key by decrypting the rebuilt encrypted session key using the regenerated key encryption key. Col. 2, line 62-col. 3, line 17. Weidong fails to teach a continuous encryption key stream, as required by claim 41, but rather teaches a set of indices based on a vector, which may be input by a user. Col. 7, lines 31-35. Nowhere does Weidong teach or suggest a fixed length segment of a continuous encryption key stream, as required by claim 41.

Since neither Medvinsky nor Weidong discloses or suggests the recited limitation and no other art of record adds the missing disclosure, accordingly, Applicants respectfully request that the rejection of claim 41 and all claims dependent thereon, be withdrawn.

Regarding claim 48, Applicants respectfully maintain that Medvinsky, alone or in combination with Weidong or other references of record, fails to teach or suggest

> a session count evaluator configured to determine if a difference between a received session count within the encrypted data packet and a locally generated session count is less than a threshold,

as required by claim 48. Medvsinky teaches synchronization by directing key stream generator 132 to output the same key stream bytes from the same key stream used to encrypt the data. Paragraph 0034. Medvinsky teaches N, which is a counter that holds the number of times that a time stamp has wrapped around. Paragraph 0042. Nowhere does Medvinsky expressly teach a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold, as required by claim 48. The Office implies that the synchronization of the stream cipher using a time stamp of Medvinsky and the counter value N of Medvinsky each inherently teach the limitations of claim 48.

Applicants respectfully point out that while a teaching may be express or inherent, inherency is a stringent standard. See In re Robertson, 169 F.3d 743, 745; 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999); MPEP § 2112.IV. Applicants disagree that it is inherent for the system of Medvinsky to practice the claim. For example, there is no teaching or suggestion that the synchronization techniques of Medvinsky must (or do) determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold, as required by claim 48. To be inherent in determining if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold, those functions must by necessity be performed in Medvinsky. They are not.

Since Medvinsky does not expressly or inherently disclose or suggest the recited limitation and no other art of record adds the missing disclosure, accordingly, Applicants respectfully request that the rejection of claim 48 and all claims dependent thereon, be withdrawn.

Regarding claim 53, Applicants respectfully maintain that Medvinsky, alone or in combination with Weidong or other references of record, fails to teach or suggest

```
selecting a fixed length segment of a continuous
encryption key stream
```

as required by claim 53. Medvinsky teaches that

> processor 124 coordinates with key stream generator 122 to begin generating a key stream based on a single key. Upon generation of the key stream, encryptor 118 encrypts each voice packet using the key stream. As noted, time stamps are employed to perform synchronization so the voice packets are recoverable at the remote end. Each voice packet includes an RTP time stamp used as a pointer to the key stream. Encryptor 118 employs the RTP time stamp to calculate an index into the key stream, and thereafter, calls key stream generator 122 to get the appropriate key stream bytes for encryption.

Paragraph 0033. Nowhere does Medvinsky teach or suggest selecting a fixed length segment of a continuous encryption key stream, as required by claim 53.

Weidong fails to compensate for the shortcomings of Medvinsky. Weidong teaches generating a session key, generating a key encryption key based on an initial vector, and generating a set of indices by a one-way transform mapping based on the length of the binary representation of the encrypted session key, the length of the binary representation of the encrypted data, and the initial vector. Col. 2, lines 39-61. Wiedong teaches regenerating the set of indices by using the one-way transform mapping based on the length of the binary representation of the encrypted session key, the length of the binary representation of the encrypted data, and the initial vector, rebuilding the encrypted session key by using the regenerated set of indices, regenerating the key encryption key, using the initial vector, and regenerating the session key by decrypting the rebuilt encrypted session key using the regenerated key encryption key. Col. 2, line 62-col. 3, line 17. Weidong fails to teach a continuous encryption key stream, as required by claim 53, but rather teaches a set of indices based on a vector, which may be input by a user. Col. 7, lines 31-35. Nowhere does Weidong teach or suggest a fixed length segment of a continuous encryption key stream, as required by claim 53.

Since neither Medvinsky nor Weidong discloses or suggests the recited limitation and no other art of record adds the missing disclosure, accordingly, Applicants respectfully request that the rejection of claim 53 and all claims dependent thereon, be withdrawn.

Claims 9-13, 28-32, 40, and 52 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Medvinsky in view of Weidong, and further in view of U.S. Patent No.

7,110,546 to Staring (hereinafter, "Staring"). Applicants respectfully maintain that claims 9-13, 28-32, 40, and 52 depend from allowable base claims and are allowable for at least this reason.

Additional Remarks

New claim 57 is added. Applicants believe that the references of record fail to teach or suggest limitations of new claim 57.

In summary, all claims are believed to be allowable over the art of record, and a Notice of Allowance to that effect is respectfully solicited. Nonetheless, if any issues remain that could be more efficiently handled by telephone, the Examiner is requested to call the undersigned at the number listed below.

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that, on the date shown below, this correspondence is being

☐ deposited with the US Postal Service with sufficient postage as first class mail in an envelope addressed as shown above.

☐ facsimile transmitted to the USPTO.

☒ transmitted using the USPTO electronic filing system.

Nicole Teitler Cave — 2/16/07
Nicole Teitler Cave — Date

EXPRESS MAIL LABEL: _____

Respectfully submitted,

Nicole Teitler Cave, Reg. No. 54,021
Attorney for Applicant(s)
(512) 338-6315 (direct)
(512) 338-6300 (main)
(512) 338-6301 (fax)